REMARKS

Reconsideration of the present application in view of the enclosed amendments and remarks is respectfully requested. Claims 23 and 41-60 have been cancelled. Claims 1-14, 16-19, 21-22, 24-34, 36-39, 61-74, and 76-79 have been amended. Claims 81-99 have been added. Claims 15, 20, 35, 40, 75, and 80 remain pending without amendment.

Claims 1, 21, 61, and 81 are the pending independent claims.

ARGUMENT

The Office Action objects to the drawings, and the Office Action includes claim rejections based on 35 U.S.C. § 103(a).

Objections to the Drawings

The Office Action objects to the original drawings because of the figures drawn by hand. This response includes formal drawings to replace the original drawings. Approval and entry of these replacement drawings is respectfully requested.

35 U.S.C. § 103(a)

The Office Action rejects claims 1-80 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent no. 5,809,546 to Paul Gregory Greenstein et al. (hereinafter "Greenstein") in view of U.S. patent no. 4,419,724 to Michael H. Branigin et al. (hereinafter "Branigin"). To the extent those rejections might be applied to the claims as amended, Applicants respectfully traverse those rejections.

The present invention pertains to firmware or other software that facilitates enhanced security and/or integrity for processing systems, and to related systems, methods, and apparatuses. For instance, claim 1 pertains to a software module known as a "processor executive" that, when executed on a processor, loads an operating system executive (OSE) in a secure environment of the platform.

By contrast, Greenstein pertains to a method for managing input/output (I/O) buffers in shared storage, and Branigin pertains to a main bus interface package. Neither Greenstein nor Branigin discloses or suggests a processor executive that, when executed on a processor, loads an operating system executive in a secure environment of a platform.

The Office Action asserts that the central processing unit (CPU) illustrated at reference number 101 in Fig. 1 of Greenstein constitutes a "processor executive." However, Greenstein's CPU clearly is not a "processor executive (PE) executable on a processor to load an operating system executive (OSE) in a secure environment," as recited in claim 1 of the present application, as amended. In fact, Greenstein's CPU is not any kind of software, let alone software that loads an OSE.

Consequently, even if Greenstein and Branigin were to be combined, the combination would not render claim 1 obvious. Further, claims 21, 61, and 81 also involve features that are similar to or the same as the feature of claim 1 described above, and all other pending claims depend ultimately from claim 1, claim 21, claim 61, or claim 81. The cited art therefore does not render any of the pending claims unpatentable.

In addition, the pending claims recite numerous additional features that are not disclosed or suggested by either Greenstien or Branigin. For example, claim 61 recites "a processor capable of selectively operating in a normal execution mode and, alternatively, in an isolated execution mode." Neither Greenstien nor Branigin discloses or suggests a processor that can switch between normal execution mode and isolated execution mode.

Claim 61 also recites a "PE supplement residing in storage within the system, the PE supplement comprising a PE manifest that represents the PE." Neither Greenstien nor Branigin discloses or suggests a PE supplement with a PE manifest that represent the processor executive. In addition, claim 61 recites "a PE handler to verify the PE using … the PE supplement." Greenstien and Branigin do not disclose or suggest any such feature.

Numerous additional features from the pending claims that are not disclosed or suggested by Greenstein and Branigin could also be noted. For instance, claim

34 involves a method with operations comprising "executing an isolated create instruction during a process of booting the platform, the isolated create instruction loading the PE handler into the isolated memory area." Further, claim 76 involves a non-interruptible atomic sequence performed by the isolated create instruction, wherein the atomic sequences includes operations such as (a) "reading a thread count register in a chipset to determine if the processor is the first processor in the isolated execution mode;" (b) "configuring the processor in the isolated execution mode;" and (c) "loading the PE handler into the isolated memory area." None of those features is disclosed or suggested by Greenstien or Branigin.

For these and other reasons, all pending claims are allowable.

FILING RECEIPT

Applicants also respectfully request a corrected filing receipt, to correct the spelling of inventor Millind Mittal's name, in accordance with MPEP §§ 605.04(b) and 605.04(g). Due to a typographical or transliteration error, the filing receipt incorrectly spells his first name as "Milland," when the proper spelling is "Millind." Enclosed herewith please find a copy of the filing receipt dated September 19, 2000, with the correction noted.

INFORMATION DISCLOSURE STATEMENTS

Applicants also request confirmation that the Examiner has considered the references listed on four information disclosure statements (IDSs) filed on (a) September 4, 2001, (b) June 14, 2002, (c) November 18, 2002, and (d) December 11, 2003, respectively. Copies of those IDSs are enclosed for reference.

The Office Action included some IDSs, but it only included one of the two pages of references filed on September 4, 2001, and the page that was included only seems to have three sets of initials, although that page lists four references.

The Office Action did not include any portion of the IDS that was filed on June 14, 2002.

The Office Action only included one of the two pages of references filed on November 18, 2002.

The IDS that was filed on December 11, 2003 lists ten references, but the copy enclosed with the Office Action has only eight sets of initials.

CONCLUSION

In view of the foregoing reasons and other reasons readily apparent, claims 1-40 and 61-99 are all in condition for allowance.

As indicated above, Applicants also request a corrected filing receipt and confirmation that all references cited by Applicants have been considered.

If the Examiner has any questions, the Examiner is invited to contact the undersigned at (512) 314-0349. Early issuance of Notice of Allowance is respectfully requested.

Respectfully submitted,

Dated: 6/7/04

MBarré

Michael R. Barré
Patent Attorney
Intel Americas, Inc.
Registration No. 44,023
(512) 314-0349

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313 on:

6.8.04
Date of Deposit

[illegible]
Name of Person Mailing Correspondence

[illegible] 6.8.04
Signature Date